

Entorno personal de aprendizaje:

Curso de Ciberseguridad: Seguridad en medios digitales



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

 **GOBIERNO
NACIONAL**

*Paraguay
de la gente*

Unidad 2. Correo Electrónico

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Viceministerio de Tecnologías de la Información y Comunicación

Director General de Inclusión Digital y TIC en la Educación

Dirección General de Ciberseguridad y Protección a la Información

SEDE 1



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

Dirección: Complejo Santos E2 - Gral. Santos 1170 c/ Concordia

Teléfono: (+595 21) 217 9000

Correo electrónico: comunicacion@mitic.gov.py

Mesa de entrada: sgeneral@mitic.gov.py

Asunción – Paraguay

Entorno personal de aprendizaje (PLE):
Curso de Ciberseguridad: Seguridad en medios digitales

Todas las imágenes presentes en este material de apoyo educativo han sido reconocidas y, en todos los casos, son de uso libre. Todas las fuentes bibliográficas utilizadas en este material de apoyo educativo son citadas mediante el gestor de referencias bibliográficas Zotero, desarrollado por el Center for History and New Media de la Universidad George Mason, utilizando el estilo de la American Psychological Association Séptima Edición.

1. Correo no deseado

1.1. Spam o correo no deseado



Denominamos spam al correo electrónico no deseado, el cual a su vez, puede ser malicioso o no malicioso. Muchas veces se trata de un correo molesto que promociona diferentes productos y servicios a través de publicidad no solicitada, enviada masivamente a las direcciones de correo de los usuarios. Este tipo de correo no deseado suele ser molesto, pero en general, no suele ser malicioso.

En otros casos, sin embargo, sus fines son maliciosos: obtener información confidencial, engañar al usuario para que ingrese a un enlace, fraude, entre otros. Constituye además uno de los principales medios de propagación de una importante cantidad de códigos maliciosos: virus, troyanos, gusanos y otros tipos de malware. En este módulo nos centraremos principalmente en este tipo de correos no deseados maliciosos.

Cuando no se siguen buenas prácticas en el uso del correo electrónico, podemos convertirnos en receptores de spam así como también en generadores de spam, es decir, nuestras cuentas de correo pueden ser utilizadas para enviar spam a otros. Esto normalmente causa enormes problemas a las organizaciones, que observan diversos síntomas como: lentitud en el servicio de correo, los correos enviados no llegan a destino, intermitencia en otros servicios, entre otros.

2. Enlaces Falsos

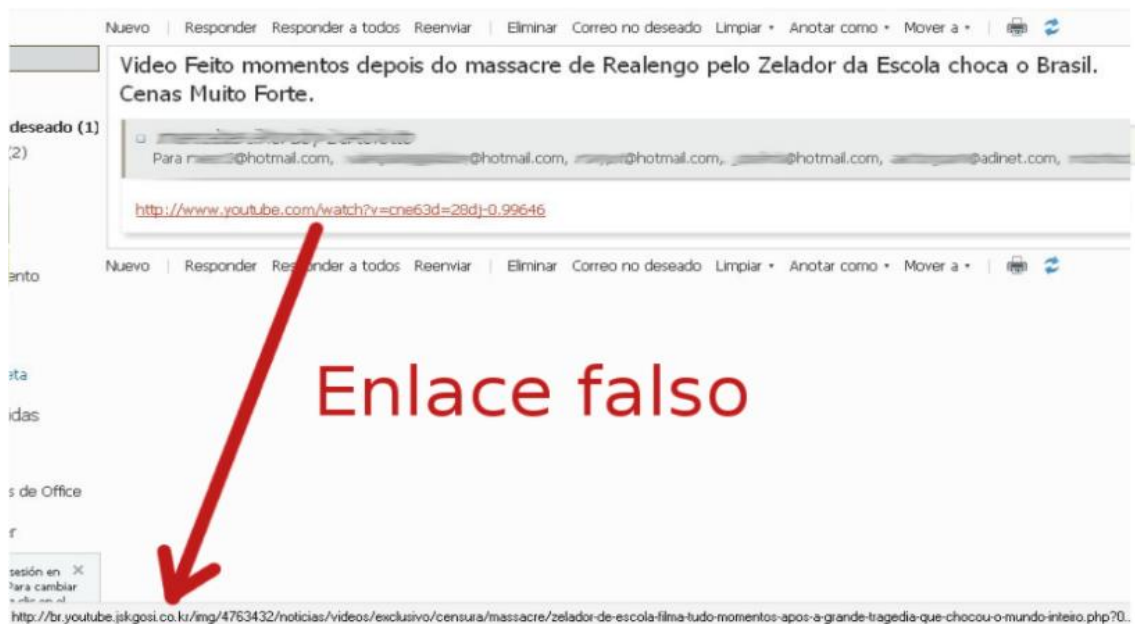
2.1. Enlaces Falsos de correos no deseados.

Cuando recibimos un correo no deseado, uno de los principales riesgos son los enlaces falsos. Muchas veces, mediante estos enlaces, buscan engañarnos de modo a que ingresemos al enlace, creyendo que nos redirigirá a un cierto sitio, sin embargo, nos redirige a otro, por lo general, falso y/o malicioso.

EJEMPLO:

En el siguiente ejemplo podemos ver un supuesto enlace a un video de YouTube, que aparentemente es: <http://www.youtube.com/watch?v=cne63d=28dj-0.99646>

A primera vista, esto parecería un enlace legítimo de YouTube, aparentemente inofensivo. Sin embargo, esto que vemos es solo un texto, que tiene el estilo de un enlace (texto rojo y subrayado) pero no es el texto del enlace real.



Unidad 2. Correo Electrónico

Para saber cuál es el enlace real al que apunta dicho texto, es necesario posicionar el puntero del mouse sobre el texto del enlace, sin hacer clic sobre él, y observar la esquina inferior izquierda de la pantalla. Allí veremos el enlace real al que apunta el texto del enlace y sabremos a donde nos llevará, una vez que hagamos clic. En este caso, vemos que el enlace real es:

<http://br.youtube.jsk.gosi.co.kt/img/4763432/noticias/videos/exclusivo/censura/massacre/zelador-de-...>, es decir, es totalmente diferente al enlace de video de YouTube que esperábamos ver.

Si vemos que el enlace real se ve sospechoso y/o corresponde a un dominio que no conocemos o no estamos seguros si queremos acceder, es mejor no hacer clic.

Y no solamente por medio de correos electrónicos, también se dan en redes sociales:

 **Superseis Supermercados**
@Superseis5

Estimados clientes: Rogamos tener cuidado con este tipo de mensajes que están llegando vía Whatsapp

MENSAJE DE ESTAFA



SUPERSEIS han anunciado que regalarán cupones de \$500 durante el estado de ...

www.superseis.com.py

SUPERSEIS está regalando cupones gratis de \$ 500 durante el estado de emergencia. Obtenga su cupón gratis en <http://superseis.cuponesonline.co>

09:08

Ante la gran cantidad de consultas sobre estos mensajes, informamos a nuestros clientes que **se tratan de publicaciones falsas que buscan estafar** aprovechándose de la buena fe de las personas. Toda acción o promoción oficial de Superseis será debidamente comunicada en nuestras redes.



 **Toyotoshi S.A.** ✓

14 de septiembre a las 20:52 · 🌐

Comunicado Importante

TOYOTOSHI S.A INFORMA

Que actualmente no posee ninguna promoción vigente que sortee vehículos de la marca Toyota en Paraguay.

Hacemos esta aclaración ya que desde las ultimas horas se está difundiendo en Redes Sociales un link invitando a participar de una **PROMOCIÓN FALSA** que regala un Toyota RAV4 Híbrido a través de la cual obtienen datos personales de los usuarios que accedan al enlace.

Instamos a nuestros clientes y seguidores a no ingresar a dicho enlace ni proporcionar sus datos personales.

Forwarded



Toyota: 90° Aniversario!

Participa y gana la nueva TOYOTA RAV4 HYBRID!

toyota.google.uno

Miraaaaa

<https://toyota.google.uno>

18:06

FALSO

 **TOYOTOSHI**
EXCLUSIVA PARAGUAY

3. Remitentes Falsos

3.1. Correos de remitentes falsos

Otro riesgo asociado a los correos electrónicos son los remitentes falsos.

Normalmente, acostumbramos a mirar el campo del remitente ("From", "De", etc.) para determinar quién nos envió el correo, ya sea mediante el nombre de dicha persona o su dirección de correo. Sin embargo, el campo del remitente no necesariamente corresponde a la persona real que nos envió el correo: tanto el nombre, como incluso la dirección de correo electrónica que vemos en dicho campo pueden ser datos totalmente falsos.

Por tanto, si por ejemplo recibimos un correo cuyo remitente es "Soporte Google <support@google.com>", no hay absolutamente ninguna garantía de que el correo sea realmente de Google (aun cuando la dirección de correo pareciera ser del dominio google.com).

EJEMPLO:

En el siguiente correo electrónico, vemos que el remitente es, aparentemente, info@amazon.com, lo que parecería ser una cuenta de correo legítima de Amazon:



Unidad 2. Correo Electrónico

Sin embargo, este no es el remitente real: si examinamos el código fuente del mensaje, podemos ver que el origen real es el servidor de correo mocha3013.mochahost.com (IP: 198.38.82.169) que, como podemos verificar, no tiene nada que ver con amazon.com.

Origen del mensaje

```
smtp.mailfrom=mocha3013.mochahost.com; hotmail.com; dkim=none (message not
signed) header.d=none;hotmail.com; dmarc=fail action=quarantine
header.from=amazon.com;
Received-SPF: None (protection.outlook.com: mocha3013.mochahost.com does not
designate permitted sender hosts)
Received: from COL004-MC5F17.hotmail.com (10.152.80.53) by
CO1NAM03FT034.mail.protection.outlook.com (10.152.80.177) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id
15.1.1101.12 via Frontend Transport; Tue, 30 May 2017 13:55:41 +0000
X-IncomingTopHeaderMarker:
OriginalChecksum:C1D688AEC63AEFC4DE1355C04C63D8B76C849AB58C38EF0A67FD49BA8B3A9878;UpperCasedChecksum:5DBAF15
51FAA766A218923702CB8DCB6385E3A9072C73A9D84A9D8DFFC4F3A90;SizeAsReceived:1346;Count:19
Received: from mocha3013.mochahost.com ([198.38.82.169]) by COL004-MC5F17.hotmail.com over TLS secured channel with
Microsoft SMTPSVC(7.5.7601.23143);
Tue, 30 May 2017 06:55:15 -0700
Received: from manuartu by mocha3013.mochahost.com with local (Exim 4.86_1)
(envelope-from <manuartu@mocha3013.mochahost.com>)
id 1dFhc9-00380r-Ov
for gabriratti@hotmail.com; Tue, 30 May 2017 08:55:14 -0500
To: <gabriratti@hotmail.com>
Subject: Has recibido un regalo de Amazon!
Content-Type: text/plain; charset="windows-1251"
From: AMAZON <info@amazon.com>
Message-ID: <E1dFhc9-00380r-Ov@mocha3013.mochahost.com>
Date: Tue, 30 May 2017 08:55:13 -0500
```

Cerrar

Por supuesto que el análisis del código fuente de un mensaje y del origen real requiere un cierto grado de conocimiento técnico, y no es una acción que vamos a realizar cada vez que recibimos un correo. No se pretende que los usuarios finales aprendan a analizar este código fuente, pero sí es importante que todos recordemos siempre que, ni el nombre ni la dirección que aparecen en el campo del remitente no son garantía de que el correo realmente haya enviado por esa persona.

Ante la duda, siempre es mejor no abrir el enlace ni el adjunto si lo hubiera y preguntar primero a alguna persona que pueda ayudarnos a determinar el origen (informático, técnico de TI, etc.), o incluso chequear con la persona que dice habernos enviado el mensaje si es que realmente lo envió.

4. Phishing

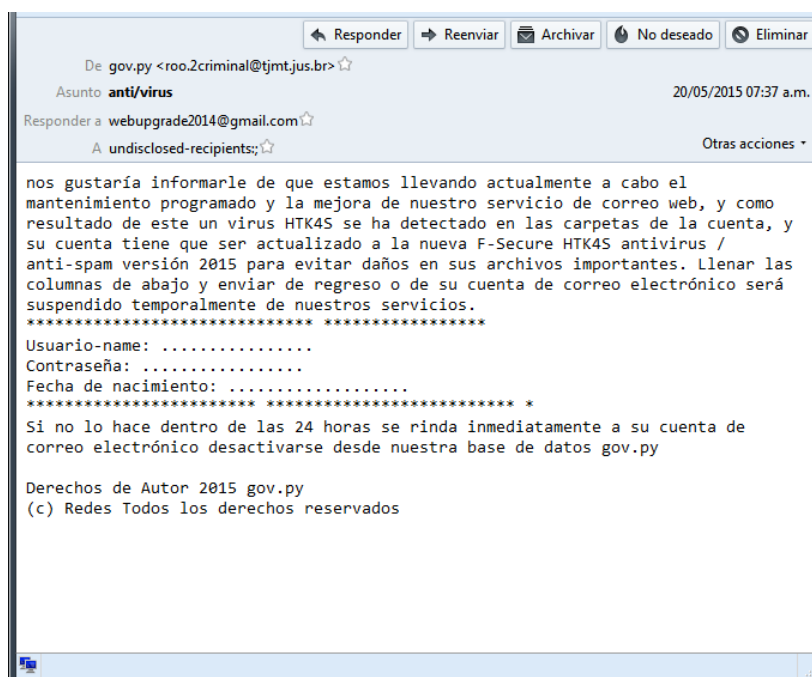
4.1. Phishing a través de Correo Electrónico



El phishing, en general, es una modalidad delictiva encuadrada en la figura de estafa o engaño realizado a través de Internet, y constituye otra de las amenazas de seguridad más propagadas a través del correo electrónico. A través de este engaño el atacante busca que la víctima le proporcione información útil o confidencial, como por ejemplo contraseñas, PIN de la tarjeta de crédito, u otro tipo de información que le puede servir a una persona malintencionada para realizar otro tipo de ataques con dicha información.

En la siguiente figura vemos un ejemplo de phishing recibido a través de un correo electrónico. En el mensaje, el atacante busca engañar a quien recibe el correo, de modo a que crea que se trata de un administrador de TI y que debe enviarle su contraseña para que éste realice unas tareas de mantenimiento.

Unidad 2. Correo Electrónico



Se trata de un engaño, de un mensaje falso: cuando la víctima responde a este correo enviando su usuario, contraseña y fecha de nacimiento, tal como se le solicita, esta información la recibirá el ciberdelincuente, quien con esto podrá acceder a la cuenta del usuario. También podría vender dicha información a otra persona que estuviera interesada en acceder a una cuenta de la víctima o realizar otros tipos de ataques relacionados.

A continuación, vemos otro ejemplo de phishing a través de correo electrónico:

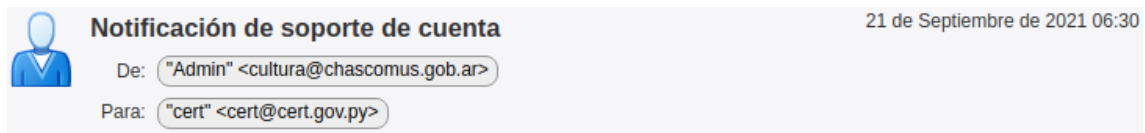
En este caso, el ciberdelincuente simula un mensaje del banco, advirtiéndonos que existe un problema con nuestro servicio bancario (en este caso, con el Token de seguridad) y que necesitamos ingresar a un enlace para revertir el problema. Como podemos ver (en la esquina inferior izquierda), el enlace corresponde a un dominio totalmente distinto al del banco, y probablemente se trata de un sitio falso, que aunque visualmente pueda ser igual al del banco, tiene como objetivo que el usuario ingrese su contraseña de modo a que ésta sea obtenida por el atacante. En el módulo de Ingeniería Social veremos ejemplos de estas páginas de phishing.

Los mensajes fraudulentos están limitados únicamente por la creatividad del ciberdelincuente: en algunos casos, el mensaje no será muy convincente y nos hará dudar; sin embargo, en otros casos el mensaje estará redactado de tal forma que nos hará creer que es

Unidad 2. Correo Electrónico

un correo legítimo. Si además se combinan técnicas de enlaces falsos y remitentes falsificados, el engaño será más difícil de distinguir, si es que no prestamos atención a todos los detalles.

Ejemplo de análisis de un correo electrónico malicioso.



ID: cert@cert.gov.py

Nos enteramos de que su correo electrónico no pasó por el proceso de verificación / actualización en el que estamos trabajando actualmente.

Actualmente estamos actualizando nuestra base de datos y el centro de cuentas de correo electrónico.

[clic aquí para continuar](#)

Nota: Es posible que sus correos electrónicos no se entreguen hasta que verifique su cuenta..

Soporte de TI © 2021. Todos los derechos reservados.

Mas ejemplos pueden verse en el siguiente artículo: <https://www.cert.gov.py/noticias/correos-electronicos-y-sitios-web-falsos-como-reconocerlos>.

5. Buenas Practicas en el uso del correo electrónico

5.1. Recomendaciones

Como vimos en las secciones previas, existen muchos riesgos y técnicas de ataque cuando hablamos de correo electrónico, entre ellos el spam (ya sea malicioso como no malicioso) y el phishing.



Algunas de las recomendaciones y buenas prácticas en el uso del correo electrónico para evitar ser víctimas y/o generadores de spam son las siguientes:

1. No confiar en correos spam con archivos adjuntos y explorar el archivo antes de ejecutarlo. Esto minimiza la posibilidad de ejecutar un malware. Se debe tener en cuenta que cualquier archivo, por más inofensivo que parezca (un pdf, documento de texto, .zip, imagen, etc) pueden contener código ejecutable escondido dentro del archivo.
2. Cuando se reciben adjuntos, prestar especial atención a las extensiones de los mismos, ya que suelen utilizar técnicas de engaño como la doble extensión (por ejemplo, un archivo con nombre file.pdf.exe, en realidad no es un pdf sino un ejecutable .exe), espacios entre el nombre del archivo y la extensión del mismo, u otras técnicas similares.

Unidad 2.
Correo Electrónico

3. Como medida de seguridad extra, bloquear las imágenes de los correos y descargarlas cuando se asegure de que el correo no es dañino.
4. Evitar publicar las direcciones de correo en sitios web de dudosa reputación como sitios pornográficos, foros, chats, entre otros. Esto minimiza la posibilidad de que la dirección se guarde en la base de datos de los spammers (cibercriminales que se dedican a enviar spam, de forma sistemática).
5. Proteger la dirección de correo utilizando una cuenta alternativa durante algún proceso de registro en sitios web y similares. Esto previene que la dirección de correo laboral sea foco del spam.
6. Utilizar filtros anti-spam que permitan el filtrado del correo no deseado. Un filtro anti-spam bien configurado puede detectar y filtrar muchos de los correos maliciosos que vimos en los ejemplos.
7. No responder jamás el correo spam. Es preferible ignorarlos y/o borrarlos, ya que si se responde se confirma que la dirección de correo se encuentra activa.
8. Cuando recibimos un correo fraudulento, es importante reportarlo como spam. La mayoría de los servicios de correo incluyen la opción de “Marcar como Spam”, “Correo no deseado” o similar.
9. Evitar el reenvío de mensajes en cadena, ya que suelen ser utilizados por spammers para recolectar direcciones de correo activas. Estas cadenas nos piden reenviar el mensaje a una cierta cantidad de contactos, incluida la persona que nos lo envió. De esta manera, se estará alargando continuamente la lista, y al final siempre estará en copia el spammer, quien conseguirá de esta manera una gran base de datos de direcciones de correo activas para enviar más spam o realizar otro tipo de ataques más peligrosos.
10. Cuando deseamos enviar un mensaje a múltiples contactos, es recomendable hacerlo siempre Con Copia Oculta (CCO) para que quien lo recibe lea solo la dirección del emisor. Esto evita que los filtros anti-spam nos incluyan en listas negras. Cuando nuestra dirección es incluida en una lista negra, por lo general se observan dificultades para enviar correos.

Unidad 2. Correo Electrónico

11. Cuando vamos a enviar un correo a muchos contactos (normalmente más de 10 ~ 15), se debe evitar incluirlos a todos como destinatarios. Para el correo masivo se deben utilizar mecanismos como listas de distribución, herramientas o servicios de telemarketing (como, por ejemplo, Mailchimp). Esto evita que los filtros anti-spam nos incluyan en listas negras.
12. Seguir buenas prácticas para las contraseñas, utilizando claves robustas, cambiándolas con periodicidad, activando la autenticación de doble factor siempre que sea posible, etc. Muchas veces alguien buscará ingresar a nuestra cuenta, no para obtener nuestra información, sino para utilizar nuestra cuenta para enviar spam desde ahí, por lo cual la protección de nuestra cuenta mediante contraseñas seguras es fundamental para evitar ser generadores de spam.



Por otra parte, también podemos mencionar algunas recomendaciones específicas para evitar ser víctimas de phishing mediante correo electrónico:

1. Tener en cuenta que las entidades financieras y otro tipo de empresas no solicitan nunca datos confidenciales a través de este medio, de esta manera se minimiza la posibilidad de ser víctima de esta acción delictiva.
2. Jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través del correo electrónico, ya que la comunicación podría ser interceptada y robada, o nuestra cuenta podría ser accedida (por

Unidad 2.
Correo Electrónico

ejemplo, porque la contraseña de nuestra cuenta de correo no era segura), con lo que, además, el atacante podrá obtener otras contraseñas que hubiéramos intercambiado por correo.

3. Desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles (contraseñas, números de tarjeta, códigos de seguridad, etc.) ya que suelen ser engaños.
4. No hacer clic sobre enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden redireccionar hacia sitios web clonados o hacia la descarga de malware. Hoy en día existen técnicas mediante las cuales se puede infectar un equipo con solo entrar a un sitio web, sin que la víctima haya descargado ni ejecutado nada de forma intencional, esto lo estudiaremos en los siguientes módulos.
5. Observar con atención el remitente del correo, no solo el nombre que figura sino también la dirección de correo. Si bien, existen técnicas que pueden camuflar completamente la dirección de correo, como vimos en la sección de Remitentes Falsos, esta medida puede protegernos en muchos casos en los que la dirección de correo es engañosa. Por ejemplo, podemos recibir un correo de info@amaz0n.com: la o fue reemplazada por 0 (cero), de modo a simular ser una dirección de correo legítima de Amazon.
6. Tener mucho cuidado con el correo que llega a la bandeja de correo no deseado. Si bien, en ocasiones el correo legítimo puede terminar en la bandeja de spam, en muchos casos el correo que se encuentra allí es malicioso. Si no estamos absolutamente seguros que es un correo legítimo, no debemos abrirlo.
7. Comunicarse telefónicamente con la persona u organización que dice ser el remitente para descartar la posibilidad de ser víctimas de un engaño, si se tiene dudas sobre la legitimidad de un correo.
8. Habituar a examinar periódicamente la actividad en las cuentas (bancarias, de correo, de redes sociales, etc.), a fin de detectar a tiempo alguna actividad extraña relacionada con la manipulación de la cuenta o transacciones no autorizadas.

Unidad 2.
Correo Electrónico

9. Estar atentos a las nuevas formas delictivas, siguiendo las noticias en sitios de seguridad.
10. Si bien, este artículo esta dirigido principalmente a correos electrónicos, tener en cuenta que puede realizarse también por otros medios, como en redes sociales, mensajes de texto y aplican los mismos cuidados.

